UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,455	11/17/2003	Kazuya Suzuki	8022-1063	2290

466 7590 06/09/2009

YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER
ZEE, EDWARD

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
06/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,455	SUZUKI ET AL.	
	Examiner	Art Unit	
	EDWARD ZEE	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendments filed on March 20th, 2009. Claim 1 has been amended; Claims 1-19 are pending and have been considered below.

Claim Objections

2. **Claim 1** is objected to because of the following informalities: the Examiner notes that as currently recited, it may be unclear and indefinite in regards to if the *"multicast packet"* positively contains said enciphered data *and* a current use key identifier. Further clarification is kindly requested. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. **Claims 1-19** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The Examiner respectfully submits that the newly introduced limitation *"said current use cipher key being separate from said current use decipher key"* does not appear to be supported by the original disclosure. The Examiner further notes that the closest relevant support appears

to be on page 103 of the specification, which is directed towards the aspect of separate keys for different multicast deliveries [lines 21-26], and not separating the cipher and decipher keys. The Applicant is kindly requested to clarify such issues by citing where support can be found in the specification and/or explaining how the specification was interpreted to provide such support.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-19 are drawn towards a multicast delivery system, which in light of at least pages 33-41 of the specification, appear to encompass a purely software embodiment. Software is not a series of steps or acts and this is not a process. Software is not a physical article or object and as such is not a machine or manufacture. Software is not a combination of substances and therefore not a compilation of matter. Thus, software by itself does not fall within any of the four categories of invention. Therefore, Claims 1-19 are not statutory.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-4, 18 and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by Caronni et al. (6,049,878).

Claim 1: Caronni et al. discloses a multicast delivery system comprising:

a. a delivery server which enciphers delivery data by using a current use cipher key to generate enciphered data and transmits a multicast packet containing said enciphered data*(ie. traffic encryption component receives IP packets...encrypts the entire IP packet...etc.)* and a current use key identifier identifies a pair of said current use cipher key and a current use decipher key as current use keys*(ie. each packet also includes a key version field and a key revision field...etc.)*, said current use cipher key being separate from the said current use decipher key*(ie. cipher key located in participant key management component of sender and decipher key located in participant key management component of receiver, or the like)* [column 5, lines 1-12 & figure 2];

b. a key management server which is connected with said delivery server through a network, holds as a current use key data, a set of said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as a current use decipherment key data in response to a current use key data request*(ie. group key manager knows a number N shared secrets, ie. keys...associated with each key is a version number and a revision number...etc.)* [column 6, lines 1-39];

c. and a client terminal*(ie. new participants or old participants which need to resynchronize)* which is connected with said delivery server and said key management server through said network, receives said multicast packet from said deliver server, issues said current use key data request*(ie. during join operations and/or participants requesting version updates if*

it appears they have missed messages) to said key management server to receive said current use decipherment key data from said key management server, holds said set of said current use decipher key and said current use key identifier*(ie. participant key management component receives information from group key management component…to obtain and maintain participant key records)*, and deciphers said enciphered data contained in said multicast packet by using said current use decipher key when said current use key identifier contained in said multicast packet is coincident with said current use key identifier held in said client terminal*(ie. traffic decryption component is the receiver of the data and inverts the operation of the traffic encryption component in the sending unit)* [column 5, lines 1-11 & 32-42 | column 6, lines 51-65 | column 10, lines 1-12].

Claim 2: Caronni et al. discloses the multicast delivery system according to claim 1, and further discloses that said delivery server generates and holds as a current use encipherment key data, a set of said current use cipher key, said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as said current use decipherment key data to said key management server, and said key management server holds said current use decipher key and said current use key identifier as said current use decipherment key data*(ie. during join operations revision numbers are increased for new participants and cause new keying material to be generated)* [column 6, lines 51-65].

Claim 3: Caronni et al. discloses the multicast delivery system according to claim 2, and further discloses that said delivery server sets a current use key remaining effective time data to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use

decipherment key data to said key management server, said key management server holds said current use decipherment key data, and said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses*(ie. receiver is only authorized for the time period for which they have paid)* [column 2, lines 10-12].

Claim 4: Caronni et al. discloses the multicast delivery system according to claim 3, and further discloses that said delivery server generates as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data, when said current use key remaining effective time data becomes a first present value, and transmits a set of said next use decipher key, said next use key identifier, and said next use key remaining effective time data to said key management server as a next use decipherment key data, and said key management server holds said next use decipher key data*(ie. older keys are thrown away after a preselected amount of time)* [column 9, lines 51-59].

Claim 18: Caronni et al. discloses the multicast delivery system according to claim 1, and further discloses that said key management server detects a data amount of said multicast packets and charges a fee to said client terminal based on said detected data amount*(ie. authorized to participate at some periods of time, etc.)* [column 2, lines 4-21].

Claim 19: Caronni et al. discloses the multicast delivery system according to claim 1, and further discloses that said client terminal issues said key data request to said key management server, and said key management server detects the number of said key data requests and charges

a fee to said client terminal based on said detected number of key data requests*(ie. pay-per-view program access)* [column 2, lines 4-21].

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 5-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni et al. (6,049,878) in view of Larsen et al. (7,068,791).

Claim 5: Caronni et al. discloses the multicast delivery system according to claim 4, and further discloses that said client terminal issues a key request to a key management server, but does not explicitly disclose that a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

However, Larsen et al. discloses a similar system and further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 6: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 5, but Caronni et al. does not explicitly disclose that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

However, Larsen et al. further discloses that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0*(ie. current key is used until it expires)* [column 4, lines 15-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 7: Caronni et al. discloses the multicast delivery system according to claim 1, and further discloses the delivery server generating current use key data, but does not explicitly disclose that said delivery server issues a current use key data generating request to said key management server, said key management server generates and holds as a current use key data, a set of said current use cipher key, said current use decipher key and said current use key identifier in response to said current use key data generating request, and transmits a set of said current use

cipher key and said current use key identifier as a current use encipherment key data to said delivery server, and said delivery server holds said current use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses that a delivery server issues a current use key data generation request to a key management server, wherein the key management server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users, as suggested by Larsen et al. [column 1, lines 33-40].

Claim 8: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 7, and Caronni et al. further discloses that said key management server sets a current use key remaining effective time data to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use encipherment key data to said delivery server, said delivery server holds said current use encipherment key data, and said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses*(ie. older keys are thrown away after a preselected amount of time)* [column 9, lines 51-59].

Claim 9: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 8, and Caronni et al. further discloses that said delivery server issues a next use key data generating request to said key management server, when said current use key remaining effective

time data becomes a first present value, said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data in response to said next use key data generating request, and transmits a set of said next use encipher key, said next use key identifier, and said next use key remaining effective time data to said delivery server as a next use encipherment key data, and said delivery server holds said next use encipherment key data*(ie. transmission of the revision number of the KEKs can be postponed until the updated keys are actually used)* [column 6, lines 60-65].

Claim 10: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 9, and Caronni et al. further discloses that said client terminal issues a key request to a key management server, but does not explicitly disclose that a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

However, Larsen et al. discloses a similar system and further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen

et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 11: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 10, but Caronni et al. does not explicitly disclose that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

However, Larsen et al. further discloses that said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0*(ie. current key is used until it expires)* [column 4, lines 15-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 12: Caronni et al. discloses the multicast delivery system according to claim 1, and further discloses a plurality of said delivery servers, but does not explicitly disclose that each of said plurality of delivery server issues a next use key data generating request to said key management server while using said current use cipher key, said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, and transmits a set of said

next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and said delivery server holds said next use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses that a delivery server issues a current use key data generation request to a key management server, wherein the key management server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Furthermore, Larsen et al. discloses a delivery server issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users and give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 1, lines 33-40 & column 4, lines 15-17].

Claim 13: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 12, but Caronni et al. does not explicitly disclose that each of said plurality of client terminals issues a next use decipher key request to said key management server when said client terminal does not hold said current use key identifier contained in said multicast packet, said key management server transmits a set of said next use decipher key and said next use key identifier

to said client terminal as a next use decipherment key data, and said client terminal holds said next use decipherment key data.

However, Larsen et al. further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 14: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 12, and Caronni et al. further discloses that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients, each of said plurality of client terminals issues a next use decipher key request to said key management server in response to said key data change previous notice, said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and said client terminal holds said next use decipherment key data*(ie. periodical change of keying material and change of revision numbers)* [column 7, lines 1-6].

Claim 15: Caronni et al. discloses the multicast delivery system according to claim 1, and further discloses:

a. a plurality of said delivery servers [column 5, lines 43-58];

b. and a plurality of said client terminals [column 5, lines 43-58];

c. a plurality of key management server [column 5, lines 43-58];

d. but does not explicitly disclose:

i. a master server;

ii. and a plurality of slave servers, wherein each of said plurality of delivery servers issues a next use key data generating request to said master server while using said current use cipher key, said master server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and transmits a set of said next use decipher key and said next use key identifier as a next use decipherment key data to said plurality of slave servers, each of said plurality of slave servers holes said next use decipherment key data, and said delivery server holds said next use encipherment key data.

However, Larsen et al. discloses a similar system and further discloses a master key server*(ie. network operator)* and a plurality of slave servers*(ie. user stations)*, wherein a delivery server issues a current use key data generation request to a master key server, wherein the master key server transmits the current use key data to the delivery server*(ie. pass key request message to the network operator station)* [abstract].

Furthermore, Larsen et al. discloses a delivery server issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is reached the user station must get the next network operator public key, however it will keep using the current key until it expires)* [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to prevent an unauthorized delivery server from interfering with legitimate users and give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 1, lines 33-40 & column 4, lines 15-17].

Claim 16: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 15, but Caronni et al. does not explicitly disclose that each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers when said client terminal does not hold said current use key identifier contained in said multicast packet, said slave server transmits said next use decipherment key data to said client terminal, and said client terminal holds said next use decipherment key data.

However, Larsen et al. further discloses that a client terminal issues a next use key request to a key management server when a current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server*(ie. when the renewal time is*

reached the user station must get the next network operator public key, however it will keep using the current key until it expires) [column 4, lines 10-17].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the system disclosed by Caronni et al. with the feature disclosed by Larsen et al. in order to give all the client terminals a chance to get the next key before the current one expires, as suggested by Larsen et al. [column 4, lines 15-17].

Claim 17: Caronni et al. and Larsen et al. disclose the multicast delivery system according to claim 15, and Caronni et al. further discloses that each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients, each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers in response to said key data change previous notice, said slave server transmits said next use decipherment key data to said client terminal, and said client terminal holds said next use decipherment key data*(ie. periodical change of keying material and change of revision numbers)* [column 7, lines 1-6].

Response to Arguments

10. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
June 6, 2009
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435